DIGITALFORENSICS QUESTIONS AND ANSWERS

Aung Zaw Myo (www.forensicsmyanmar.com)

Digital Forensics Quizs

Digital Forensics (1-100) အမေးအဖြေ အချို့သည် India ရာဇသတ်ကြီး၊ သက်သေခံဥပဒေ၊ India နှင့် Global အခြေအနေဖြင့် မေးမြန်းဖြေဆိုထားခြင်းဖြစ်ပါသည်။

#Question

Digital Forensics Professional တစ်ယောက်ဖြစ်ဖို့ Field ကိုဝင်ရောက်ဖို့ Bachelor Or Master ဘွဲ့တွေလိုအပ်ပါသလား ?

#Answer

ဒီအမေးကိုဖြေရမယ်ဆိုရင် မလိုအပ်ပါဘူးလို့ပဲ ဖြေပါရစေ။ Digital Forensics မှာ ကျွမ်းကျင်သူတွေများစွာလိုအပ်ပါတယ်။ ဒါပေမဲ့ ဘွဲ့ မရတဲ့သူတွေက Professional မဖြစ်နိုင်ဘူး ဒီ Field ကို မဝင်ရောက်နိုင်ဘူးလို့ မဆိုလိုပါဘူး။ အလုပ်တစ်ခုအတွက် ဘွဲ့ဆိုတာ Gate Pass တစ်ခုပဲဖြစ်ပါတယ်။ Bachelor Or Master တွေရရှိထားပေမဲ့ Professional လို့ မသတ်မှတ်နိုင်ပါဘူး။ Digital Forensics Field ကိုဝင်ရောက်ဖို့ Professional Cerifitcation တွေ Course တွေ ဒီအချိန်မှာ ရှိနေပါပြီ။ Digital Forensics Filed ကိုဝင်ရောက်ဖို့ဆိုရင် နည်းပညာကိုဝါသနာပါမှုနဲ့ Analysis Skill ရှိဖို့လိုအပ်ပါတယ်။ အလုပ်အနေနဲ့ ပြောရရင် First Responder, Lab Assistant လိုနေရာမျိုးတွေက Analysis Skill ရှိဖို့မလိုအပ်ပါဘူး။ သူတို့အလုပ်က သိမ်းဆည်းဖို့၊ စာရွက်စာတမ်းပြုလုပ်ဖို့၊ Imaging လုပ်ဖို့ပဲဖြစ်ပါတယ်။တစ်ဖက်ကပြောရရင် Digital Forensics Brachelor ဘွဲ့က Certification တွေထက်သာပါတယ်။ Certification Course တွေကတော့ Deep Knowledge အနေနဲ့ သီအိုရီရော လက်တွေ့ပိုင်းရော ရနိုင်ပါတယ်။

ဒါပေမဲ့ သူကအပိုင်းနဲ့သူကတော့ ရှိစမြဲပါ အလုပ်ဝင်ဖို့၊ ရာထူးတိုးဖို့ဆိုရင်တော့ ဘွဲ့၊ Professional Certificate ၊ အတွေ့အကြုံ၊ ဝါသနာ၊ Research and Development၊ ပါးနပ်မှု၊ ပေါင်းသင်းဆက်ဆံမှု၊ အင်တာဗျူး အခြေအနေ စတာတွေနဲ့ပဲ အခြေခံဆုံးဖြတ်ပါတယ်။ အနှစ်ချုပ်အနေနဲ့ ဒီ Field ကိုဝင်ရောက်ဖို့ဘွဲ့တွေက အဓိက မကျပါဘူး။ ဒါပေမဲ့ Professional ဖြစ်ဖို့အတွက်ဆိုရင် reskill နဲ့ upskill ကတော့ အရေးကြီးပါတယ်။

#Question

Qualification မရှိပဲနဲ့ Expert Witness ဖြစ်နိုင်ပါသလား ?

#Answer

Globally မှာ Expert Witness ဖြစ်ဖို့အတွက် သတ်မှတ်ထားတာတွေ မရှိပါဘူး။ Digital Forensic Professional သို့မဟုတ် ကျွမ်းကျင်တဲ့ ဘယ်သူမဆို လုပ်နိုင်ပါတယ်။ ဒါပေမဲ့ တရားရုံးဆိုတာ စံ သတ်မှတ်ချက်ရှိတာကြောင့်

Digital Forensics Expert Witness လုပ်မဲ့သူက Computer/IT နဲ့ပတ်သတ်တဲ့ ဘွဲ့တစ်ခုခုနဲ့ Forensics Course တစ်ခုခု တက်ရောက်ထားသင့်ပါတယ်။ နည်းပညာက လျှင်မြန်စွာပြောင်းလဲနေတဲ့ အတွက်ဖြစ်ပါတယ်။ Indian Context အရ Expert ဆိုတာ

An expert is a person
who has devoted time and study to a special branch of learning, and thus, is especially skilled on t hose points on which he is asked to state his opinion. Under

45 Section 45 of the Indian Evidence Act, 1872 expert means one who is a #specially skilled person

#Question

Open source forensics tools / frameworks တွေက Digital Forensics မှာ Analysis လုပ်ဖို့အတွက် အဆင်ပြေလုံလောက်မှုရှိပါသလား ? တရားရုံးကရော လက်ခံနိုင်ပါသလား ?

#Answer

Evidence တစ်ခုထဲကိုပဲ တူညီတဲ့ အခြားသော Forensics Tools တွေနဲ့လဲ ရရှိနိုင်ပါတယ်။ open source tools / frameworks တွေသုံးစွဲလို့ တရားရုံးက လက်မခံတာမရှိသေးပါဘူး။ open source tools / frameworks နဲ့ပတ်သတ်ပြီး license , Original Equipment Manufacturer (OEM) , Tools က ဘယ်လိုအလုပ်လုပ်တယ်ဆိုတာနဲ့ ပတ်သတ်ပြီး မေးမြန်းရာမှာ မဖြေဆိုနိုင်ခဲ့တာရှိပါတယ်။ (open source tools / frameworks သုံးမယ်ဆိုရင် license , Original Equipment Manufacturer (OEM) , Tools က ဘယ်လိုအလုပ်လုပ်တယ်ဆိုတာ သိရမှာ ဖြစ်ပါတယ်) Commercial Tools တွေလိုပဲ open source tools / frameworks တွေက Evidences ရှာရာမှာ တော်တော်လေး အသုံးဝင်ပါတယ်။ ဒါကြောင့်

Commercial Tools တွေအပြင် open source tools / frameworks တွေကိုလဲ သုံးစွဲနိုင်ပါတယ်။ သုံးစွဲမယ်ဆိုရင် Report မှာ ထည့်သွင်းဖော်ပြရမှာ ဖြစ်ပါတယ်။

#Question

Digital Forensics Lab တည်ထောင်ဖို့အတွက် ဘယ်လို Standard တွေကို သိထားသင့် ဖတ်ထားသင့်ပါသလဲ ?

#Answer

ISO/IEC 17025:2017 - General requirements for the competence of testing and calibration laboratories.

(ISO/IEC,
2017)ISO /IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.

(ISO/IEC, 2012)ISO/IEC 27041 :2015- Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method. (ISO/IEC, 2015)

ISO/IEC 27042:2015 - Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence.

(ISO/IEC,
2015)ISO/IEC 27043:2015 - Information technology — Security techniques — Incident investigation principles and processes. (ISO/IEC, 2015)

#Question

MD5 Hash က အားနည်းချက်ရှိတဲ့ အတွက် Digital Forensics မှာ Integrity Check အတွက် မသုံးသင့်ဘူးလို့ ပြောနေကြပါတယ်။ သင့်ရဲ့အမြင်ကရော ? ဖြေရှင်းချက်ကရော ?

#Answer

MD5 (128 bit) နဲ့ SHA1(160 bit) ကို Digital Forensics မှာ Integrity Check အတွက် အဓိကထားပြီးသုံးစွဲပါတယ်။ Collision attack ကြောင့် MD5 နဲ့ SHA1 မှာ အားနည်းချက်ရှိတာကို သက်သေပြချက်တွေအရ သိထားပါတယ်။ Digital Forensics မှာ Hash Function ကို သုံးစွဲရတာက Encryption အတွက် သုံးစွဲတာမဟုတ်ပါဘူး။ Integrity Check အတွက်သာ သုံးစွဲတာ ဖြစ်ပါတယ်။

#Question

Digital Forensics Professional တစ်ယောက်က Cyber Law ကိုသိသင့်ပါသလား ? သိသင့်တယ်ဆိုရင် ဘာလို့သိသင့်တာလဲ ?

#Answer

မေးခွန်းကိုဖြေမယ်ဆိုရင် သိသင့်သလို မသိရင်လဲ ရတယ်လို ဖြေချင်ပါတယ်။ ဒါပေမဲ့ သိသင့်တယ်ဆိုတာကို နည်းနည်းဖောင်းပေးပြီး ပြောပါရစေ။ Digital forensics ဆိုတာက techno-legal field ဖြစ်တာကြောင့် Forensics Report ကိုရေးသားပြင်ဆင်သူက တရားရုံးမှာ သက်သေထွက်ဆိုရမှာ ဖြစ်တာကြောင့် Cyber Law ကိုသိရပါမယ်။ Digital Forensics Professional တစ်ယောက်က Law ကို လုံးဝမသိဘူးဆိုတာမဖြစ်သင့်ပါဘူး။ အခြားသော ဥပဒေတွေထဲကမှ Cyber Law ကို ကျွမ်းကျွမ်းကျင်ကျင် သိသင့်ပါတယ်။ Digital Forensics Professional တစ်ယောက်က သူ့ရဲ့တာဝန် အလုပ်နဲ့ ကျင့်ဝတ်တွေကို သိသင့်ပါတယ်။ ဒါမှသာ ပြင်ပအဖွဲ့အစည်း သို့မဟုတ် အစိုးရဘက်မှာ Investigation လုပ်တော့မယ်ဆိုရင် Law ကို သိထားခြင်းဖြင့် ပိုပြီးအဆင်ပြေနိုင်ပါတယ်။ Digital Forensics Professional တစ်ယောက်အနေနဲ့ opinion (ထင်မြင်ယူဆချက်) ပေးတဲ့အခါမှာ တရားရုံးမှာ ပြန်လှန်မေးခွန်းမေးတဲ့အခါမှာ Law ကို သိထားရင် ပိုပြီး အဆင်ပြေနိုင်ပါတယ်။ ဒါမှသာ ကိုယ့်ရဲ့ opinion ကို အများသိအောင် ပြောကြားနိုင်မှာဖြစ်ပါတယ်။ တစ်ကယ်တန်းပြောရရင် Cyber Law သာမက အခြားသော

ပတ်သတ်ဆက်နွယ်နေတဲ့ ဥပဒေတွေကိုပါသိထားသင့်ပါတယ်။ ဒါမှ ကိုယ်စစ်ဆေးတဲ့ Evidences တေထဲမှာ အကျုံးဝင်လာခဲ့ရင် ကိုယ့်အတွက်ပို အဆင်ပြေမှာ ဖြစ်ပါတယ်။ Law ကို လုံးဝမသိဘူးဆိုရင် DF Professional တစ်ယောက်အနေနဲ့ အဆင်မပြေနိုင်ပါဘူး။ DF Professional ရဲ့ အဓိက တာဝန်က Case နဲ့ပတ်သတ်တာကို Analysis လုပ်ရုံပဲဖြစ်ပါတယ်။ သူ့ Professional က ဥပဒေထက် နည်းပညာ ကျွမ်းကျင်မှုက ပိုပြီး အဓိက ကျပါတယ်။ ကျွမ်းကျင်မှုရှိမှသာ Evidence တွေကို Analysis လုပ်နိုင်မှာ ဖြစ်ပါတယ်။ နည်းပညာ တိုးတက်လာမှုကြောင့် စိမ်ခေါ်မှု များစွာက Digital Forensics Field မှာသာမက investigators နဲ့ judiciary ပိုင်းမှာပါ ရှိနေပါတယ်။ Cyber Law ကျွမ်းကျင်မှု နည်းပညာ ကျွမ်းကျင်မှု တွေက စိန်ခေါ်မှု အဖြစ်ရှိနေမှာပါ။ AI အသုံးချမှု များလာတာကြောင့် AI နဲ့ ပတ်သတ်တဲ့ Cyber Law တွေ Investigation နဲ့ Cyber Law မှာ AI အသုံးချတာတွေ လိုအပ်လာပါလိမ့်မယ်။

Digital Forensics Professional တစ်ယောက် အနေဖြင့် တရားရုံးတွင် သက်သေခံရန်အတွက် ပြင်ဆင်ရန် အချက်များ

Digital Forensic Analyis ပြုလုပ်ရာမှာ အဓိက လိုက်နာရမည့် အချက်အချို့မှာ

၁။ Analysis လုပ်ထားပြီးသော အချက်အလက်များကို မလွဲမှား မပျောက်ပျက် စေရန်။

၂။ မူရင်း Evidence Devices ပေါ်တွင် မည်သည့်အခါမှ စစ်ဆေးခြင်း မပြုလုပ်ရန်။

၃။ စစ်ဆေးနေစဉ်အတွင်း လိုင်စင်ရှိသော digital forensic Tools များကိုသာ အသုံးပြုရန်။

(Open Source အသုံးပြုပါက အသုံးပြုသော Tools အကြောင်း အချက်အလက်များကို စစ်ဆေးသုံးစွဲရန်။)

၄။ စစ်ဆေးနေစဉ်အတွင်း ပတ်ဝန်းကျင်မှ မည်သူ့ကိုမျှ မယုံကြည်ရန်။

၅။ စတင်စစ်ဆေးချိန်မှ စတင်ပြီး စစ်ဆေးသမျှ အဆင့်တိုင်းကို Document ပြုလုပ်ရန်။

၆။ ဥပဒေကို သေချာသိရှိရန်။

ကြုံတွေ့နိုင်သည့် အမေး အဖြေများ

#Question

Digital Forensics နဲ့ပတ်သတ်တဲ့ qualifications နဲ့ experience တွေက ဘာတွေလဲ ?

#Answer

ရရှိထားသောဘွဲ့။ Digital Forensics နှင့်ပတ်သတ်သော Certificate/Course , အတွေ့အကြုံ

#Question

ယခု Forensics Report ကို ကိုယ်တိုင်ရေးသားတာလား (သို့မဟုတ်) Evidences Analysis လုပ်ရာမှာ ကိုယ်တိုင် ပြုလုပ်တာလား ? မည်သူကရေးသားပြီး (သို့မဟုတ်) မည်သူက စစ်ဆေးတာလဲ

 # Answer

Opinion ကို ကောင်းကောင်း ပေးနိုင်ခြင်း ရှိ၊မရှိ မေးမြန်းတာ ဖြစ်သောကြောင့်

ရေးသားသူ (သို့မဟုတ်) စစ်ဆေးသူ ဖြစ်ကြောင့် ရှင်းလင်းရန်။

#Prosecution_Lawyer #Question

ယခု Forensics Report ကို ရေးသားသူ စစ်ဆေးသူ ဘယ်သူလဲ။ Report ပေါ်က လက်မှတ်က ရေးသားသူရဲ့ လက်မှတ် မှန်ကန်ပါသလား ?

#Answer

မူရင်းလက်မှတ် မှန်ကန်ကြောင်း သက်သေပြရန်

#Question

Cyber Law အကြောင်းနဲ့ ယခု Case နဲ့ ပတ်သတ်တဲ့ Law အကြောင်းကို ကောင်းစွာ သိပါသလား ?

#Answer

ကျွမ်းကျင်မှု ရှိ မရှိ ဖြေဆိုရန်

#Question

Evidence ကို Lab သို့ သယ်ဆောင်လာပုံ၊ Lab မှာ Analysis ပြုလုပ်ပုံကို ရှင်းလင်းပြနိုင်မလား ?

#Answer

Evidence Report Form နှင့် Chain Of Custody (COC) Form ထဲတွင်ပါဝင်ပြီး ဖြစ်ကြောင်း ရှင်းလင်းရန်။

နောင်လာနိုင်မည့် မေးခွန်း အဖြေများတွင် ဖြေဆိုမှုနှင့် Report ထဲတွင် ပါဝင်တာ ထပ်တူကျရန်။

#Question

Mobile Phones Analysis ပြုလုပ်ပုံကို ရှင်းလင်းပြနိုင်မလား ?

#Answer

Evidence Report Form ထဲတွင် စစ်ဆေးပုံ Opinion နှင့် စစ်ဆေးသော Forensis Tool အကြောင်းပါဝင်ပြီး ဖြစ်ပါသည်။ နောင်လာနိုင်မည့် မေးခွန်း အဖြေများတွင် ဖြေဆိုမှုနှင့် Report ထဲတွင် ပါဝင်တာ ထပ်တူကျရန်။

#Question

Evidence Report က မှန်ကန်ပါတယ်လို့ သင့်ဘက်က ပြောနိုင်ပါသလား ?

#Answer

ခိုင်မာစွာ ပြောနိုင်ပါတယ်။

#Defence_Lawyer #Question

#Question

စစ်ဆေးနိုင်ရန် အတွက် Digital Forensis Lab က အဆင့်အတန်း မှီပါသလား ?

#Answer

Lab ရဲ့ Standard နှင့် Lab အတွက် ရထားသော ထောက်ခံချက်များ ပြသရန်

#Question

Evidence ရဲ့ integrity ကို မှန်ကန်ကြောင်း ပြသနိုင်ပါသလား ?

#Answer

Integrity နှင့် ပက်သတ်ပြီး Forensics Report ထဲတွင်ပါဝင်ပြီး ဖြစ်ပါတယ်။

#Question

Original Evidence Devices တွေကို စစ်ဆေးပြီး ဘယ်လို ထိန်းသိမ်းထားရှိသလဲ ? မူရင်းကို ယခု တင်ပြနိုင်မလား ?

#Answer

Imaging ပြုလုပ်ပြီးနောက်ပိုင်း ထိန်းသိမ်းထားရှိပုံကို ဖြေဆိုရန်

#Question

စစ်ဆေးနေစဉ် ဘယ်လို Tools မျိုးကို အသုံးပြုသလဲ လိုင်စင်ရော ရှိပါသလား ?

#Answer

Forensics Report ထဲတွင် မည်သည်ကို သုံးထားသည်ကို အသေးစိတ် တွေ့နိုင်ပါသည်။

#Question

သုံးစွဲထားတဲ့ Tools ကို ဘယ်လိုယုံကြည်လို့ ရနိုင်မလဲ ?

#Answer

အခြားသော Tools ဖြင့် Evidence ရရှိထားပုံကို ပြသရန် (သို့ မဟုတ်) အခြားသော Tools ဖြင့် စစ်ဆေးခံနိုင်ကြောင်း ပြောရန်

3-3-2021 နယူးဒေလီ India National Cyber Forensics laboratory ၏ ခေါင်းဆောင် Mr. Khadsare နှင့် ForensicsFocous အင်တာဗျူး

Question

Mr. Khadsare အနေနဲ့ Cyber Security နဲ့ Digital Forensics မှာ နှစ်ပေါင်း 20 လောက် လုပ်ကိုင်ခဲ့တဲ့အတွက် ဒီလမ်းကြောင်းကို ဘယ်လိုရောက်ရှိလာပါသလဲ ? India နိုင်ငံအနေနဲ့ ဒီအပိုင်းတွေမှာ တိုးတက်လာမှုအပေါ်ဘယ်လိုမြင်ပါသလဲ ?

Answer

1999 မှာ Pune University ကနေ electronics and telecommunication engineer ဘွဲ့ရရှိခဲ့ပါတယ်။ အစပိုင်းမှာ communications , networking. အပိုင်းမှာ အလုပ်လုပ်ကိုင်ခဲ့ပါတယ်။ investigation အပိုင်းမှာ စိတ်ပါဝင်စားတာကြောင့် Pune University မှာ ဖွင့်လှစ်တဲ့ Asian School of Cyber Laws ကနေ Crime Investigation Course ကိုတက်ရောက်ခဲ့ပါတယ်။ ဒီ Course ကနေ စတင်ခဲ့ပြီး နောက်ပိုင်းမှာ Forensics အပိုင်းကိုပဲဇောက်ချလုပ်ကိုင်ခဲ့ပါတယ်။ Digital Forensics နဲ့ပတ်သတ်တဲ့ Course တွေ 15 ခုလောက်ပြီးတဲ့ အခါမှာ တစ်ကယ့် Case တွေကို လုပ်ကိုင်ဖို့ အခွင့်အရေးတွေရရှိလာခဲ့ပါတယ်။ digital forensics professional တစ်ယောက်အတွက် လက်တွေ့ပိုင်းက အလွန်ပင်အရေးကြီးပါတယ်။

technology နဲ့ electronic device တွေကိုကြည့်ခြင်းအားဖြင့် digital forensics အပိုင်းမှာ တိုးတက်လာတယ်လို့မြင်ပါတယ်။ အရင်တုန်းက floppy disks, computers ,

laptops တွေကို စစ်ဆေးနေခဲ့ရာမှ အခုအခါမှာတော့ smart TVs, drones, စတာတွေ ပေါ်လာပါတယ်။ နည်းပညာအမြင်အရ ကြည့်မယ်ဆိုရင် အရင်သုံးနေကြ Storage (HHD) ထက် solid state devices (SSD) တွေကို ပိုမိုသုံးလာကြပါတယ်။ India မှာတော့ တိုးတက်မှုနှေးကွေးနေပေမဲ့ လွန်ခဲ့တဲ့ 5 နှစ်ထက်စာရင် ပိုမိုများပြားလာပါတယ်။ နောင် ၅ နှစ်မှာ India ဟာ digital forensic professionals အပိုင်းမှာ ကမ္ဘာကို ဦးဆောင်နိုင်လိမ့်မယ်လို မြင်ပါတယ်။

Question

အခုအလုပ်လုပ်နေတဲ့လုပ်ငန်းမှာ ဘယ်အပိုင်းကို ပိုစိတ်ဝင်စားလဲ ? ဘာကြောင့်လဲ ?

Answer

လက်ရှိမှာ နယူးဒေလီမှာရှိတဲ့ National Cyber Forensics laboratory ကို ဦးစီးလုပ်ကိုင်နေပြီး ကျွန်တော်အနေနဲ့Lab နဲ့ပတ်သတ်တဲ့ လုပ်ငန်းစဉ်တွေဖြစ်တဲ့ Lab ကို အဆင့်မြှင့်တင်ခြင်း၊ တိုးတက်အောင်ဆောင်ရွက်ခြင်း၊ လက်ရှိ Case တွေကို စစ်ဆေးခြင်းနဲ့ Expert Witness အဖြစ်တရားရုံးမှာ သက်သေထွက်ဆိုခြင်း စသည့် အပိုင်းတွေမှာ တာဝန်ရှိပါတယ်။ လက်ရှိအလုပ်ရဲ့အဆင့်အနေနဲ့ရော အရင်အတွေ့အကြုံတွေအရရော နောက်ပိုင်းမှာ digital/cyber forensics နယ်ပယ်မှာပဲ ဆက်လက်ပြီး လုပ်ကိုင်သွားမှာပါ။

Digital Forensics lab အနေနဲ့ Mobile Forensics အတွက် JTAG, ISP,Chip off, Micro Read စတဲ့အပိုင်းတွေမှာ အာရုံစိုက်နေပါတယ်။ Digital Forensics lab တိုင်းမှာ Computer Forensics, Mobile Forensics အပိုင်းမှာ ကန့်သတ်ချက်တွေ လုပ်ကိုင်နိုင်စွမ်းတွေရှိပါတယ်။ နောက်ထက် cloud forensics , network forensics အပိုင်းတွေကိုလဲ ထပ်မံလုပ်ဆောင်နေပါတယ်။ လက်ရှိမှာ IoT/IIoT

forensics, SCADA forensics, drone forensics, automotive forensics, blockchain forensics အပိုင်းတွေကိုလဲ တိုးတက်အောင် လုပ်ဆောင်နေပါတယ်။

ကျွန်တော်အမြင်အရ အရေးအကြီးဆုံးအပိုင်းက capacity building အပိုင်းပဲဖြစ်ပါတယ်။ digital/cyber forensics အပိုင်းမှာ လုပ်ကိုင်မဲ့သူတွေ မရှိတာတွေရှိပါတယ်။ Lab တွေများပြားလာတာနဲ့အမျှ အလုပ်အကြွေးတွေကို လျှော့ချဖို့ လိုလာပါတယ်။ Analysis လုပ်တဲ့အပိုင်းကို တိုးမြှင့်လိုလာပါတယ်။

Question

နောင် 10 စုနှစ်တစ်ခုအတွင်း India မှာရှိတဲ့ digital forensics examiner တွေအတွက် စစ်ဆေးမှုအပိုင်းမှ ဘယ်လို စိန်ခေါ်မှုတွေရှိလာနိုင်မလဲ ? ဘယ်လိုအလုပ်မျိုးတွေ ဒီလို စိန်ခေါ်မှုတွေကို ဖန်တီးသလဲ ?

Answer

စိန်ခေါ် မှုတွေကတော့ India တင်မဟုတ်ပဲ တစ်ကမ္ဘာလုံးဖြစ်မှာပါ။ ကျွန်တော်အနေနဲ့ အပိုင်းလိုက်ခွဲပြီး ပြောမယ်ဆိုရင်

Classical Problems ဖြစ်တဲ့Digital Device တွေများပြားလာသည့်ပြဿနာရယ် ။Device တိုင်းမှာ Storage ပမာဏ များပြားလာတဲ့ ပြဿနာ တွေပဲဖြစ်ပါတယ်။ ဒါတွေကြောင့် စစ်ဆေးရမဲ့ ပမာဏတွေ များပြားပေမဲ့ စစ်ဆေးမှု အပိုင်းမှာ ရရှိတဲ့အချိန်နည်းပါးပါတယ်။

Skilled Manpowerအပိုင်းမှာလဲ လိုအပ်တဲ့အရည်အချင်းနဲ့ကိုက်ညီတဲ့ သူတွေရှားပါးပါတယ်။ သူ့အပိုင်းအလိုက် အပိုင်းလိုက်မှာ ကွဲပြားတဲ့ အရည်အချင်းတွေလိုအပ်ပါတယ်။ဥပမာ။ Storage Media Forensics , Mobile Forensics လုပ်နေသူရဲ့ ကျွမ်းကျင်မှုက drone Forensics ဒါမှမဟုတ် SCADA forensics အပိုင်းမှာ မကျွမ်းကျင်နိုင်ပါဘူး။ Lab မှာလဲ ဆိုင်ရာအပိုင်းအလိုက် lab assistant, Lab analyst, Lab quality manager, Lab technical manager အစရှိသည်ဖြင့်ရှိပါတယ်။ ဒါတွေအပေါ်မူတည်ပြီး ကျွမ်းကျင်မှုတွေ ကွဲပြားပါတယ်။ digital forensics labs,law enforcement agencies, judiciary တွေမှာ ကျွမ်းကျင်သူနည်းပါးတာတော့ ရှိနေမှာပါ။

Digital Forensic Tools တွေနဲ့ပတ်သတ်ပြီး Lab မှာ အသုံးပြုတဲ့ tools တွေက ဈေးအလွန်ကြီးတာကြောင့် တက္ကသိုလ်တွေမှာ သင်ကြားရေးအတွက် အသုံးမပြုနိုင်ပါဘူး။ Open Source Tools တွေရှိပေမဲ့ လက်တွေ့မှာ အသုံးမပြုနိုင်ပါဘူး။ Forensics commercial tools တွေအတွက် သင်တန်းက ဈေးကြီးတဲ့ အတွက် အသက်မွေးဝမ်းကြောင်းအဖြစ် ရွေးချယ်သူတွေ နည်းပါးပါတယ်။

Cyber Law နဲ့ပတ်သတ်ပြီးပြောရရင် boundary-less ဖြစ်ပေမဲ့ globally အရ လက်ခံတဲ့ ဥပဒေမျိုး တရားစီရင်မှုမျိုး မရှိသေးပါဘူး။ digital forensics Case နဲ့ပတ်သတ်ပြီး တူညီမှုတွေရှိပေမဲ့ နိုင်ငံတိုင်းက စုံစမ်းစစ်ဆေးတာတွေ မတူညီကြပါဘူး။

Evolving Technologies ပတ်သတ်ပြီးပြောရရင် solid state devices, IoT/IIoT, SCADA, drones စတာတွေ တွေပေါ်လာတာကြောင့် digital forensic investigation ပုံစံလဲပြောင်းလဲ သွားပါတယ်။ Artificial intelligence ကိုdigital forensics မှာ အသုံချနိုင်ပါတယ်။ ဒါပေမဲ့ Analysis အတွက်မှာတော့ AI ကို အစားထိုးအသုံးချလို့မရနိုင်ပါဘူး။

အခြားစိန်ခေါ်မှုကတော့ Anti-Forensics နည်းလမ်းတွေကို အသုံးချလာတာကြောင့်ဖြစ်ပါတယ်။ နောက်တစ်ခုကတော့ Case ပြီးပေမဲ့ စစ်ဆေးတဲ့ Log တွေကို 3 လကြာထားရတာက Lab အတွက်အခက်အခဲဖြစ်ပါတယ်။ အချိန်လျှော့ချသင့်ပါတယ်။

Question

Digital Forensics Experts တွေတင်မက Lab မှာ လုပ်မဲ့သူတွေ စစ်ဆေးသူတွေ ရှေ့နေတွေ တရားသူကြီးတွေကို လူစွမ်းအားအရင်းအမြစ်တိုးတက်ဖို့အတွက် india မှာဘယ်နေရာကနေ လုပ်ဆောင်နေပါသလဲ ?

Answer

Forensics နဲ့ပတ်သတ်ပြီး Digital India Program အောက်ကနေလုပ်ဆောင်နေပါတယ်။ နောင်လာမဲ့ကမ္ဘာမှာ Cyber နည်းပညာမရှိပဲ မဖြစ်လာနိုင်ပါဘူး အခုအချိန်က စပြီးခြေလှမ်းလှမ်းဖို့ စတင်သင့်တဲ့အချိန်ပါပဲ။ india မှာရှိတဲ့ များစွာသောတက္ကသိုလ်တွေမှာ Postgraduate ရော Graduate အတန်းတွေမှာ digitalforensics ကိုထည့်သွင်းသင်ကြားနေပြီးဖြစ်ပါတယ်။ India , Gandhinagar, Gujart မှာ National Forensics Science University (NFSU) ရှိပြီး အဲဒီကနေ Digital Forensics ကိုသင်ကြားပေးနေပါတယ်။ အဲဒါအပြင် Central Forensics Science Laboratory (CFSLs) တွေများစွာရှိပြီး အဲဒီ Lab တွေကနေ Digital Forensics Investigation အတွက် ကူးညီပေးနေပါတယ်။ အစိုးရရဲ့ Ministry Of Electronic and Information Technology ကနေ Information Technology Act 2000 အရ Lab တွေကို Examiner Of Electronic Evidence (EEE) အဖြစ် အသိအမှတ်ပြုထားပါတယ်။ Lab တွေက အတင့်အတန်းသတ်မှတ်ချက်တွေ ဥပဒေတွေကို လိုက်နာရမှာဖြစ်ပါတယ်။ အခုအချိန်မှာ Digital Forensics ၈ ခုကို တရားဝင်အသိအမှတ်ပြုထားပြီးဖြစ်ပါတယ်။ အသိအမှတ်ပြုဖို့တင်ထားတဲ့ Lab တွေလဲ အများကြီးရှိပါတယ်။ Digital Forensics နဲ့ပတ်သတ်ပြီး Awareness Program တွေကိုလဲ Law Enforcement ရှေ့နေ တရားသူကြီးတွေကို ပေးနေလျှက်ရှိပါတယ်။

Question

Forensics Focus Reader တွေကို Mr ရဲ့ Linkedin မှာ ဝေမျှတဲ့ #25Day25Questions ပတ်သတ်ပြီး ဖော်ပြခဲ့ပါတယ်။ Social Media ပေါ်မှာရှိတဲ့ Digital Forensics Community အပေါ် သင့်အနေနဲ့ အရေးပါတယ်လို့ ဘယ်လိုမြင်ပါသလဲ ?

Answer

အရင်မေးခဲ့တဲ့မေးခွန်းတွေမှာ ပြောခဲ့တဲ့အချက်တွေအရ Professional တွေက Digital Forensics Field ကို ဝင်ရောက်ဖို့ ချီတုံချတုံဖြစ်နေပါတယ် Social Media ပေါ်မှာ Community လုပ်ခြင်း အမေးအဖြေတွေပြုလုပ်ခြင်းဖြင့် အခွင့်အလမ်းတွေရရှိနိုင်ပါတယ်။

လူတွေက Digital Forensics ကို Carreer အဖြစ်လုပ်ကိုင်နိုင်မယ်ဆိုတာ သိတဲ့သူနည်းနေပါတယ်။ Digital Forensics အတွက် အလုပ်အကိုင် နေရာတွေ အသင့်ရှိနေပါတယ်။ဒီအပိုင်းနဲ့ပတ်သတ်ပြီး Diploma ကနေ Post Graduation အထိတက်ရောက်နိုင် အတွေ့အကြုံယူနိုင်ပါတယ်။

Question

Digital Forensics Professional တွေအနေနဲ့ တစ်ယောက်နဲ့ တစ်ယောက် Social Media ကနေ ဘယ်လိုရင်းနှီးမှု ဆက်သွယ်မှု လုပ်နိုင်မလဲ ? လမ်းညွှန်ပေးတဲ့သူ လေ့လာလိုသူအနေနဲ့ရော ?

Answer

Social Media တင်မကပဲ Digital Forensics Professional တွေက အခြားသောနည်းလမ်းတွေနဲ့လဲ လုပ်ဆောင်နိုင်ပါတယ်။ ဥပမာပြောရရင် Technical Magazine တွေမှာရေးသားတာမျိုး Blog ရေးတာမျိုး

Conference တွေတက်ရောက်တာမျိုး တစ်ယောက်နဲ့တစ်ယောက် အကြံဉာဏ်ပေးတာမျိုး အတွေ့အကြုံဝေမျှတာမျိုး လုပ်နိုင်ပါတယ်။

ကျွန်တော်အနေနဲ့တော့ လမ်းညွှန်ပေး အကြံဉာဏ်ပေးတာမျိုးက ပိုပြီးကောင်းပါတယ်။ Field ကိုစိတ်ဝင်စားသူတွေ လမ်းကြောင်းရွေးချယ်ဖို့ လုပ်သူတွေအတွက် အကူအညီဖြစ်ပါတယ်။ Professional Discussion တွေ Challenge တွေကနေ အတွေ့အကြုံတွေရရှိနိုင်ပါတယ်။ Case တိုင်း စစ်ဆေးမှုမတူညီနိုင်တဲ့အတွက်ဖြစ်ပါတယ်။

Question

အခုလို (ဆရာ) လမ်းညွှန်အကြံဉာဏ်ပေးလိုတဲ့အခြားသော Professional တွေ အတွေ့အကြုံနည်းပါသူတွေကို ဘယ်လိုအကြံဉာဏ်ပေးလိုပါသလဲ ? လေ့လာသူတွေကိုရော ဘယ်လို အကြံဉာဏ်ပေးလိုပါသလဲ ?

Answer

ဒါက အရေးကြီးတဲ့ မေးခွန်းပါပဲ။ ဆရာလုပ်တယ်ဆိုတာ အနုပညာတစ်ခုပါပဲ Professional တိုင်းမလုပ်နိုင်ပါဘူး။ ကျောင်းသားတွေအတွက်အချိန်ပေးနိုင်ရမယ် သူတို့ပြောတာကို နားထောင်

နိုင်ရမယ် သူတို့ကို လမ်းညွှန်ပေးနိုင်ရမယ်။ သူတို့ရဲ့ ပန်းတိုင်ရောက် အောင်ကူညီပေးနိုင်ရမယ်။ လေ့ကျင့်ခန်းတစ်ခုပေးရင်လဲ ဘယ်လိုလုပ်ရမယ်ဆိုတာမပြောပဲ လိုချင်တဲ့ Results ကိုပြောပြပြီး သူတို့ကို ရှာဖွေခိုင်းရမယ်။

အခုအချိန်မှာ သင်ဟာ သင်ကြားဖို့အတွက် ဆရာရှာနေပြီးဆိုကတည်းက သင်ဟာ ပထမဆုံးမှန်ကန်တဲ့ လမ်းကြောင်းတစ်ခုအပေါ်ရောက်နေပါပြီ။ Digital Forensics မှာ လမ်းညွှန်ပြသပေးမဲ့ ဆရာက အမြဲတမ်းလိုအပ်ပါတယ်။ သူက ရွေးချယ်ရမဲ့ Course တွေကို လမ်းညွှန်ပေးရုံမက သင် အခက်အခဲကြုံလာရင်လဲ ကူညီနိုင်ရပါမယ်။ နောက်ပြီး သင်ရဲ့အရည်အချင်းနဲ့ပတ်သတ်ပြီး အခြားသူတွေကို ပြောပြနိုင်ရပါမယ်။ ဒါက Digital Forensics Community မှာအရေးအကြီးဆုံးဖြစ်ပါတယ်။

ကျွန်တော် အမြဲတမ်းပြောနေကြ စကားရှိပါတယ်။

Digital Forensics မှာအရေးအကြီးဆုံးက

"Mentorship and Intership" ဖြစ်ပါတယ်။

Question

အလုပ်ပြီးတဲ့နောက် အားလပ်ချိန်တွေမှာ ဘာလုပ်ရတာကို နှစ်သက်ပါသလဲ ?

Answer

အချိန်ရရင် Cyber Security Digital Forensics နဲ့ပတ်သတ်ပြီး စကားပြောရ ဆွေးနွေးရတာကို နှစ်သက်ပါတယ် အချိန်အများစုကတော့ အလုပ်ထဲမှာ Digital Forensics နဲ့ပတ်သတ်ပြီး သင်ကြားပေးပါတယ်။ ကျွန်တော်နဲ့သိတဲ့သူတွေကို Social Media ဒါမှမဟုတ် Email ကနေလဲ ဖြေကြားပေးပါတယ်။ Information Security Digital Forensics နဲ့ ပတ်သတ်ပြီး ပြည်တွင်း ပြည်ပတွေမှာ စာတမ်းတွေ ရေးသားဖြန့်ဝေပါတယ်။

ယခုရေးသားမှုကိုမေးမြန်းသူနှင့် ဖြေကြားသူထံမှ ခွင့်ပြုချက်ရယူပြီး ဖြစ်ပါသည်။